REMARKS

Reconsideration of the application is respectfully requested for the following reasons:

1. Interview

The Examiner is thanked for the courtesy extended during a personal interview on July 26, 2005.

During the interview, it was agreed that amendment of the claims, to more clearly recite that the disguised operation is different than the original operation, would distinguish the Kocher patent, although the Examiner would still need to perform an update search and consider other references of record. The amendments listed above are believed to be in accord with the Examiner's comments during the interview.

2. Rejection of Claims 1-18 Under 35 USC §102(e) in view of U.S. Patent Publication No. 2001/0053220 (Kocher)

This rejection is respectfully traversed on the grounds that the Kocher publication does not disclose or suggest, whether individually or in common with any other reference of record, a data carrier having a semiconductor chip with a memory and operating program that disguises an operation h and its input x in order to obtain a disguised operation h_{RI} ***different from operation h*** and disguised input data in which:

$$h_{RI}(\text{disguised input data}) = y = h(x)$$

holds true, *i.e.*, in which performing the different operation on the disguised input data has the same effect as performing the original operation on the undisguised input data.

Instead of performing a disguised operation on disguised input data, Kocher only teaches disguising of the input data by splitting the original input data into two parts, and performing the same operations on the two parts of the input data. The operation performed on the disguised input data is thus the **same DES operation** as would have been performed on the original data,

albeit performed in two parallel operations on the respective parts of the input data using split parts of the original key. Kocher does not teach disguising of the DES operation in the manner claimed, but only the input data and the DES keys.

The method described in the Kocher publication involves enhancing DES encryption by splitting a message M and a key K into permutated message components PM1 and PM2, and permutated key components PK1 and PK2, respectively, such that PM1 $\otimes$ PM2 = M and PK1 $\otimes$ PK2 = K holds (see paragraph [0035] of the Kocher publication). Thereafter, the two message/key pairs (PM1,PK1) and (PM2,PK2) are DES-encrypted separately instead of the standard pair (M,K), so that the resulting ciphertexts can be recombined to obtain the same ciphertext that is obtained when encrypting the original message M with the original K (as explained in paragraph [0036] of the Kocher publication. Thus, it holds that:

$$DES(PM1,PK1) \diamond DES(PM2,PK2) = DES(M,K)$$

where $\diamond$ symbolizes the recombination operation. The Examiner will note that there is no attempt to perform a disguised operation on the input in order to obtain the same output values that would be obtained if the original operation were performed on the original data, but only a splitting of data and keys, which has the effect of disguising the original data.

Because the Kocher publication does not disclose or suggest disguising **both** input data and an operation performed on the input data, resulting in a **different operation** being applied to the **different input data**, it is respectfully submitted that the Kocher publication does not anticipate or suggest the claimed invention, and withdrawal of the rejection of claims 1-18 under 35 USC §102(e) is respectfully requested.

Having thus overcome each of the rejections made in the Official Action, withdrawal of the rejections and expedited passage of the application to issue is requested.

Respectfully submitted,

BACON & THOMAS, PLLC

By: BENJAMIN E. URCIA
Registration No. 33,805

Date: August 26, 2005

BACON & THOMAS, PLLC
625 Slaters Lane, 4th Floor
Alexandria, Virginia 22314

Telephone: (703) 683-0500

NWB:S:\Producer\beul\Pending Q...Z\WATER 763621\a04.wpd